

RECEIVED

OCT - 3 2016

**U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS**

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION**

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

GLOBAL ACCESS TECHNICAL SUPPORT LLC,
also d/b/a Global S Connect, Yubdata Tech, and
Technolive, a Missouri limited liability company;

GLOBAL SMIND LLC, also d/b/a Global S
Connect, a Missouri limited liability company;

SOURCE PUNDIT LLC, also d/b/a OneSource
Tech Support, a Missouri limited liability company;

HELIOS DIGITAL MEDIA LLC, a Missouri
limited liability company;

VGLOBAL ITES PRIVATE LIMITED, an Indian
corporation;

RAJIV CHHATWAL, individually and as an owner
or officer of Global Access Technical Support LLC,
Helios Digital Media LLC, and Source Pundit LLC;

RUPINDER KAUR, individually and as an owner
or officer of Global sMind LLC, and

NEERAJ DUBEY, individually and as an owner or
officer of Helios Digital Media LLC and VGlobal
ITES Private Limited.

Defendants.

Case No. _____

[FILED UNDER SEAL]

**COMPLAINT FOR PERMANENT
INJUNCTION AND OTHER
EQUITABLE RELIEF**

Plaintiff, the Federal Trade Commission ("FTC") for its Complaint alleges:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain temporary, preliminary, and permanent injunctive

relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

3. Venue is proper in this district under 28 U.S.C. § 1391(b)(2)-(3), (c)(1)-(3), and (d), and 15 U.S.C. § 53(b).

PLAINTIFF

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

5. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. § 53(b).

DEFENDANTS

Corporate Defendants

6. Defendant Global Access Technical Support LLC, also d/b/a Global S Connect, Yubdata Tech, and Technolive ("GATS"), is a Missouri limited liability company with its principal places of business at 559 Graeser Road, Creve Coeur, Missouri 63141, and 10756 Trenton Avenue, St. Louis, Missouri 63132. GATS transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or

in concert with others, GATS has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

7. Defendant Global sMind, also d/b/a Global S Connect (“Global sMind”), is a Missouri limited liability company with its principal place of business at 7923 Forsyth Boulevard, St. Louis, Missouri 63105. Global sMind transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, Global sMind has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

8. Source Pundit LLC, also d/b/a OneSource Tech Support (“Source Pundit”), is a Missouri limited liability company with its principal place of business at 559 Graeser Road, St. Louis, Missouri 63141. Source Pundit transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, Source Pundit has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

9. Helios Digital Media LLC (“Helios”) is a Missouri limited liability company with its principal place of business at 559 Graeser Road, St. Louis, Missouri 63141. Helios transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, Helios has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

10. Defendant VGlobal ITES Private Limited (“VGlobal”) is an Indian corporation with its principal place of business at 575, Block C, Sarita Vihar Colony, Delhi, South Delhi, DL 110076 India. VGlobal transacts or has transacted business in this district and throughout the

United States. At all times material to this Complaint, acting alone or in concert with others, VGlobal has advertised, marketed, distributed, or sold computer security or technical support services throughout the United States.

Individual Defendants

11. Defendant Rajiv Singh Chhatwal is an owner, officer, director, member, or manager of corporate defendants GATS, Source Pundit, and Helios. At all times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint.

Defendant Chhatwal organized and created corporate defendant GATS, contracted with its call center located in New Delhi, India, and established and maintains corporate bank and merchant processing accounts for the U.S.-based corporate defendants GATS, Global sMind, Source Pundit, and Helios. He is the domain registrant for several websites used to facilitate Defendants' telemarketing scheme. He responds to consumer complaints and corresponds with the Better Business Bureau on behalf of corporate defendants GATS and Global sMind, and in such correspondence refers to himself as their "President." He further has described himself as "owner" of GATS, "owner" and "president" of Source Pundit, "partner" and "member" of Global sMind, and "co-owner" and "president" of Helios on various bank documents, including signature cards. Defendant Chhatwal resides in this district and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

12. Defendant Rupinder Kaur is an owner, officer, director, member, or manager of corporate defendant Global sMind. At all times material to this Complaint, acting alone or in concert with others, Defendant Kaur has formulated, directed, controlled, had the authority to

control, or participated in the acts and practices set forth in this Complaint. Among other things, Defendant Kaur organized and created defendant Global sMind, and established and maintains the corporate bank and merchant processing accounts used by that entity to facilitate Defendants' telemarketing scheme. In opening the Global sMind accounts, Kaur listed herself as the sole "member" of that LLC. Defendant Kaur resides in this district and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

13. Defendant Neeraj Dubey is an owner, officer, director, member, or manager of corporate defendants Helios and VGlobal. At all times material to this Complaint, acting alone or in concert with others, Defendant Dubey has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant Dubey controls the operations of corporate defendant VGlobal, including its call center and the collection of payments from its consumer victims. Defendant Dubey established and maintains at least one bank account for corporate defendant Helios. In opening that account, he represented himself to be a "co-owner" of Helios along with Rajiv Chhatwal. In connection with the matters alleged herein, Defendant Dubey transacts or has transacted business in this district and throughout the United States.

14. Defendants GATS, Global sMind, Source Pundit, Helios, and VGlobal (collectively "Corporate Defendants") have operated as a common enterprise while engaging in the deceptive and unlawful acts and practices alleged below. The Corporate Defendants have conducted the business practices described below through an interrelated network of companies that have common ownership, business functions, office and telemarketing locations, and that have commingled funds. They share mailing addresses, business websites, telephone numbers,

and employees when soliciting consumers and dealing with third parties. Because the Corporate Defendants have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below. Defendants Chhatwal, Kaur, and Dubey have formulated, directed, controlled, had the authority to control, or participated in the acts and practices of the Corporate Defendants that constitute the common enterprise.

COMMERCE

15. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS’ BUSINESS ACTIVITIES

Overview

16. Defendants operate a telemarketing scheme that deceives consumers into purchasing unnecessary technical support or computer security services to address purported problems with their computers, regardless of whether problems with their computers actually exist. Since at least 2013, Defendants have bilked millions of dollars from consumers throughout the United States. In carrying out their scheme, Defendants employ pop-up ads that warn consumers that their computers have been hacked, infected, or otherwise compromised, and are in immediate need of computer security or technical support service. The pop-ups advise consumers to call a toll-free number to obtain that service, and mislead consumers into believing that they are contacting technical support providers affiliated with Microsoft, Apple, or other well-known companies. Instead, when consumers call, they reach Defendants’ telemarketing boiler room in India, where they are then subjected to Defendants’ deceptive and high pressure sales tactics.

Defendants' Pop-up Advertisements

17. Defendants cause pop-up messages ("pop-ups") to be displayed on consumers' computers instructing them to immediately call a toll-free number for technical support. The U.S.-based Defendants use affiliate marketers to place the pop-up advertisements, and they pay the affiliate marketers a commission based on the number of leads or calls generated from consumers seeking technical support.

18. Defendants' pop-ups warn consumers that their computers may be compromised by security threats and instruct them to call a toll free number listed in the message. The pop-ups are designed to appear as if they originated from the computer's operating system and often mislead consumers into believing that they are receiving a message from Microsoft, Apple, or their Internet service provider. The pop-ups claim that a serious technical or security issue has been identified with the consumer's computer, and provide a toll-free number that the consumer is urged to call immediately to resolve the issue. Often a loud alarm or voice recording warning of the security risk accompanies the pop-up, adding to the urgency of the message.

19. Defendants' pop-ups are typically designed so that consumers are unable to close or navigate around them, rendering consumers' web browser unusable. This practice is known as "browser hijacking."

Defendants Frighten and Deceive Consumers into Buying Unnecessary Computer Technical Support Services

20. Consumers who call the numbers contained in the pop-up message are connected to Defendants' telemarketers in India. Defendants' telemarketers then lead the consumers

through a sales pitch designed to convince them that their computers are in urgent need of repair, even though Defendants have not detected that an actual problem exists. Defendants' telemarketers begin this deception by explaining that consumers receive the pop-up messages only if something is wrong with their computers.

21. To gain consumers' trust, Defendants claim that they are affiliated with Microsoft or Apple, or otherwise certified or authorized by those companies to service their products. For example, one telemarketer told an FTC investigator that he and the other telemarketers are certified by Microsoft and Apple to service their products. In fact, Defendants and their telemarketers are not affiliated with, or certified or authorized by, Microsoft or Apple.

22. After convincing consumers that the pop-ups indicate that there are problems with their computers and that Defendants are qualified to diagnose those problems and fix them, Defendants' telemarketers tell consumers that they need to remotely access the consumers' computers to identify and resolve the specific problems. The telemarketers typically direct consumers to go to a website, enter a code, and follow the prompts to begin the remote access session. Once Defendants gain remote access, they are able to control the consumers' computers. Among other things, Defendants can view the computer screen, move the mouse or cursor, enter commands, run applications, and access stored information. At the same time, consumers can see what Defendants are seeing and doing on their computers.

23. Once in control of consumers' computers, Defendants run a series of purported diagnostic tests, which, in reality, are nothing more than a high-pressured sales pitch designed to scare consumers into believing that their computers are corrupted, hacked, otherwise compromised, or generally performing badly. For computers running versions of Microsoft Windows, these diagnostic tests often include displaying the computer's Event Viewer, the

Microsoft System Configuration Utility (“msconfig”) services tab, and the msconfig start-up menu.

24. To convince consumers that there is a problem that needs to be repaired, Defendants often show consumers numerous “Error” and “Warning” messages in the computer’s Event Viewer. For example, Exhibit A is a screenshot of an FTC computer, taken during an undercover transaction conducted on June 29, 2016, showing Defendants’ use of the Event Viewer. While displaying this screen, the telemarketer drew FTC staff’s attention to a number of errors and warnings in the computer and claimed that these are evidence of computer problems. In fact, the FTC computer used during this undercover transaction was free of viruses, spyware, malware, or other security issues at the time of the undercover transaction.

25. Defendants also use the computer’s System Configuration to show consumers that computer problems purportedly have caused a number of Windows services to stop working. For example, Exhibit B is a screenshot of the same FTC computer, taken from the same June 29, 2016 undercover transaction, showing Defendants’ use of the System Configuration. The telemarketer prompted the System Configuration window to show a number of such “Stopped” services. The telemarketer told the FTC investigator that this was a problem, because it meant his services were not in “running condition.”

26. In truth, it is impossible to know whether a computer is infected with malware, is being hacked, or is otherwise compromised based solely on the fact that the computer’s Event Viewer contains “Error” and “Warning” messages, or the fact that the System Configuration lists a number of “Stopped” services. In fact, it is normal for a Windows system to collect hundreds or thousands of “Error” or “Warning” messages in the course of normal operations over time.

Similarly, it is normal for Windows services that are not needed to be designated as “Stopped,” and this in no way indicates that there is a problem on the system.

27. Defendants nevertheless use these innocuous “Error,” “Warning,” and “Stopped” messages to scare consumers into believing that their computers are not operating properly and are in urgent need of repair.

28. Defendants charge consumers approximately \$200 for a “one-time fix” of the purported problem, or approximately \$400 for a one-year technical support plan.

29. Consumers who do not agree, or hesitate, to pay for the computer security and technical support services Defendants recommend are subjected to intense pressure. Defendants’ telemarketers will, for example, warn such consumers that by failing to purchase the recommended services, they will continue to encounter problems with their computers. In pressuring consumers to purchase the more expensive one-year subscription, Defendants’ telemarketers emphasize that the one-time fix leaves computers vulnerable to future problems, and that without a one-year contract, consumers will incur additional costs to address those problems.

30. If a consumer agrees to pay, Defendants’ telemarketers ask the consumer to provide a credit card number or, more recently, a bank account number in order to process an electronic check. Consumers’ payments are processed by banks in the United States and the funds are deposited in the accounts of the U.S.-based Defendants.

31. After charging consumers for technical support services, Defendants then spend one to two hours logged on to consumers’ computers to perform the purported “repairs.” In numerous instances, these “repairs” are unnecessary or even harmful. At best, Defendants leave consumers’ computers in no worse condition than when the consumers first called Defendants.

At worst, Defendants' services may cause consumers' computers to be more vulnerable to security incursions and other technical problems.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

32. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

33. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

**COUNT I
Deceptive Misrepresentations**

34. In numerous instances, in connection with the marketing, offering for sale, or selling of computer security and technical support services, Defendants represent or have represented, directly or indirectly, expressly or by implication, through a variety of means, including telephone calls and internet communications, that they are part of or affiliated with well-known U.S. technology companies, such as Microsoft or Apple, or are certified or authorized by these companies to service their products.

35. In truth and in fact, Defendants are not part of or affiliated with these U.S. technology companies, nor are Defendants certified or authorized to service their products.

36. Therefore, Defendants' representations set forth in Paragraph 34 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

**COUNT II
Deceptive Misrepresentations**

37. In numerous instances, in connection with the marketing, offering for sale, or selling of computer security and technical support services, Defendants represent or have

represented, directly or indirectly, expressly or by implication, through a variety of means, including through telephone calls and Internet communications, that they have detected security or performance issues on consumers' computers, including viruses, spyware, malware, or the presence of hackers.

38. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 37, Defendants have not detected security or performance issues on consumers' computers.

39. Therefore, Defendants' representations as set forth in Paragraph 37 are false, misleading, or were not substantiated at the time they were made and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

CONSUMER INJURY

40. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

41. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

PRAYER FOR RELIEF

Wherefore, Plaintiff, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the Court's own equitable powers, requests that the Court:

A. Award Plaintiff such preliminary injunctive and ancillary relief as may be necessary to avert the likelihood of consumer injury during the pendency of this action and to preserve the possibility of effective final relief, including but not limited to, temporary and preliminary injunctions, and an order providing for immediate access, the turnover of business records, an asset freeze, the appointment of a receiver, and the disruption of domain and telephone services;

B. Enter a permanent injunction to prevent future violations of the FTC Act by Defendants;

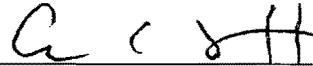
C. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

D. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Dated: October 3, 2016

Respectfully submitted,

DAVID C. SHONKA
Acting General Counsel



Elizabeth C. Scott
Illinois Bar Number: 6278075
Samantha Gordon
Illinois Bar Number: 6272135
Federal Trade Commission, Midwest Region
55 West Monroe Street, Suite 1825
Chicago, Illinois 60603
escott@ftc.gov
sgordon@ftc.gov
(312) 960-5609 [Scott]
(312) 960-5623 [Gordon]

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION